Inter-VLAN Routing

Cabrillo College

CIS 187 Multilayer Switched Networks

CCNP 3 version 4

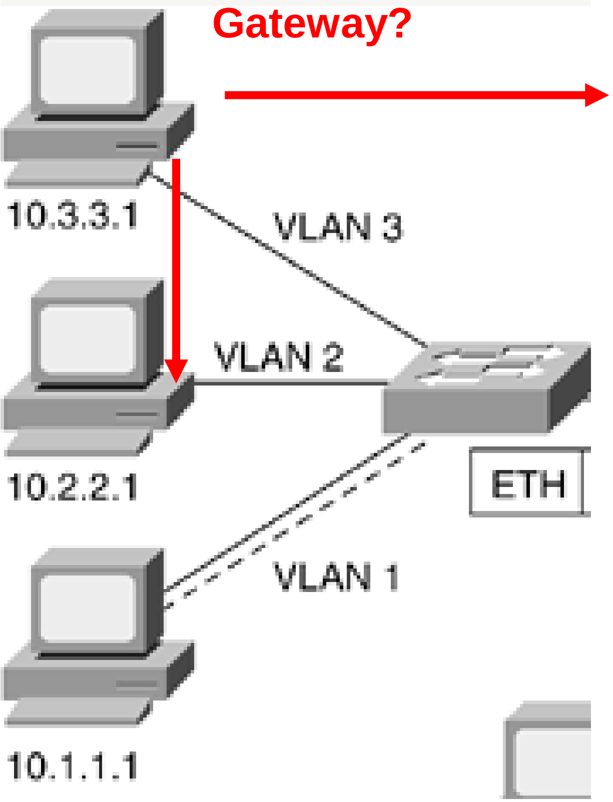
Rick Graziani

Fall 2006

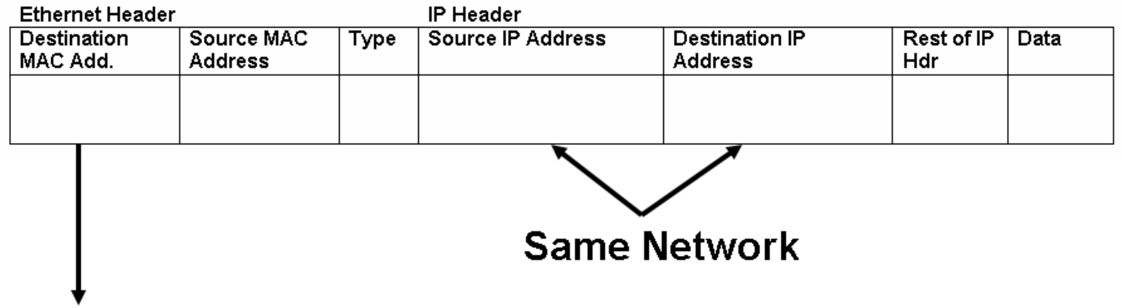
Internetwork Communications

- Even though hosts on different VLANs may be physically connected to the same switch, logically the are on separate networks.
- Remember, a host determines if it can communicate directly with another host by ANDing its own source IP address and subnet mask, determines its network address, and then ANDing the destination IP address of the packet and its own subnet mask.

Direct to host or via Gateway?



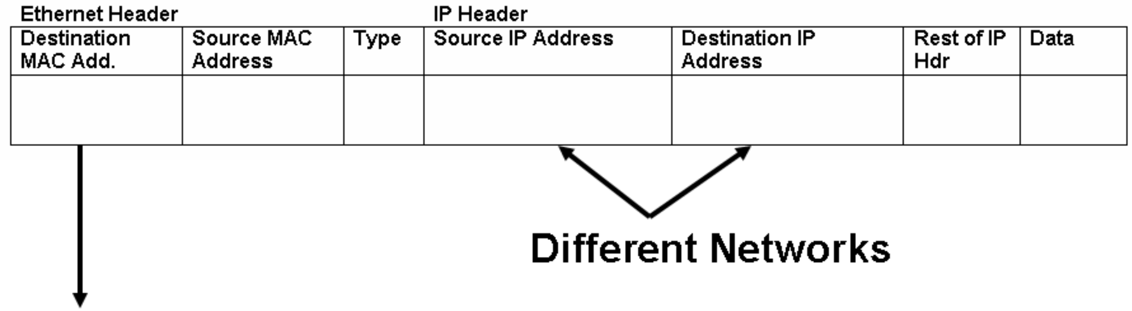
Internetwork Communications



Ethernet Header			IP Header			
Destination MAC Add.	Source MAC Address	Type	Source IP Address	Destination IP Address	Rest of IP Hdr	Data

Same Network

- Then Destination MAC Address is that of the same device as the Destination IP Address.
- Check ARP cache for entry of Destination IP Address and its MAC Address.
  - If no entry, ARP Request Destination IP Address asking for MAC Address.



Ethernet Header			IP Header			
Destination MAC Add.	Source MAC Address	Type	Source IP Address	Destination IP Address	Rest of IP Hdr	Data

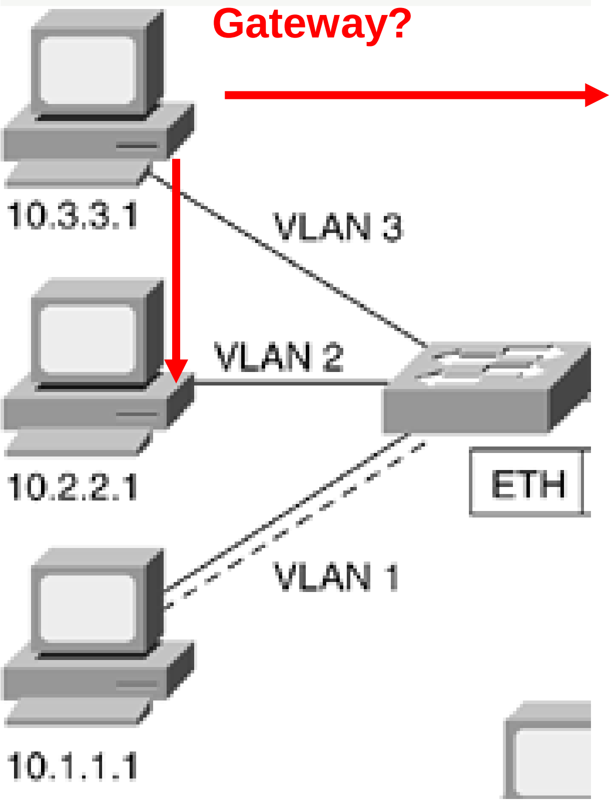
Different Networks

- Then Destination MAC Address will be that of the Default Gateway.
- Check ARP cache for entry of Default Gateway’s IP Address and its MAC Address.
  - If no entry, ARP Request Default Gateway’s IP Address asking for MAC Address.

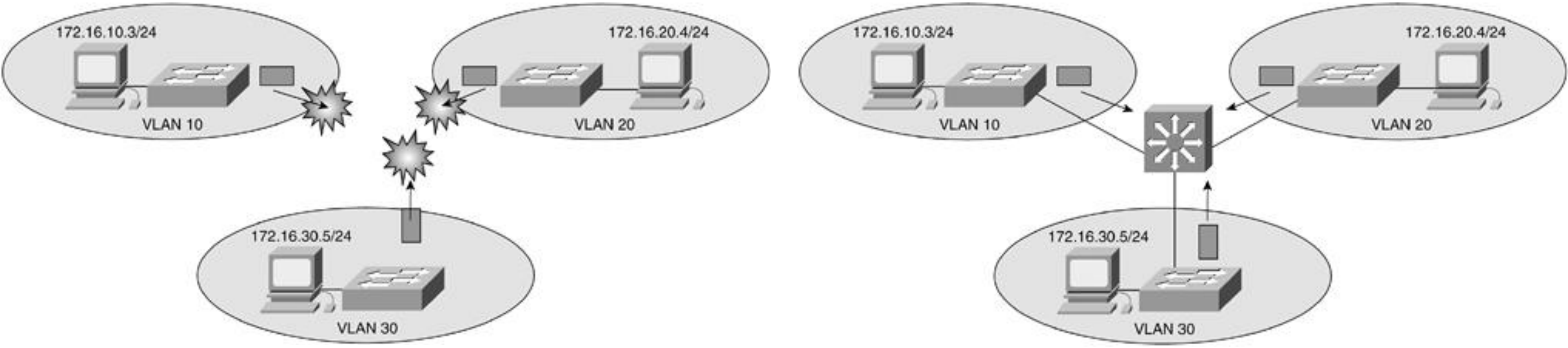
Internetwork Communications

- If the addresses match, the two hosts are on the same network and the IP packet can be encapsulated in an Ethernet frame with the destination MAC address of the same host with that destination IP Address.
- If the addresses do not match, the two hosts are on different networks.
  - The packet must be encapsulated in an Ethernet frame with the destination MAC address that of the default gateway.

Direct to host or via Gateway?



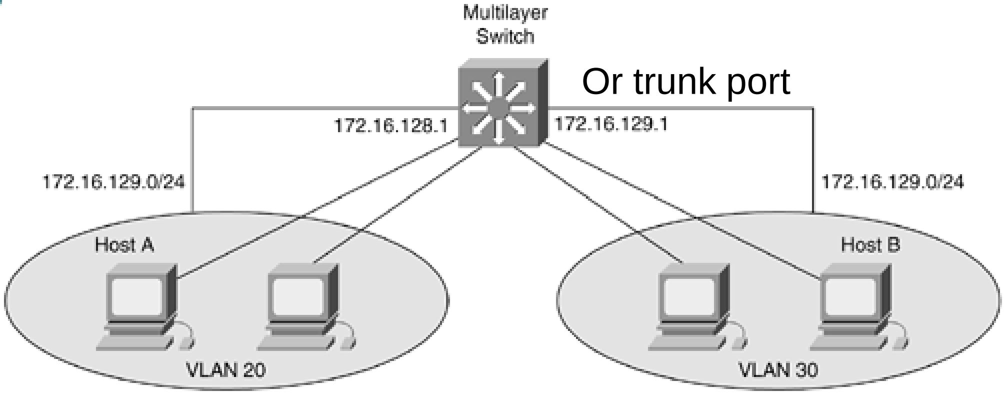
Inter-VLAN Routing



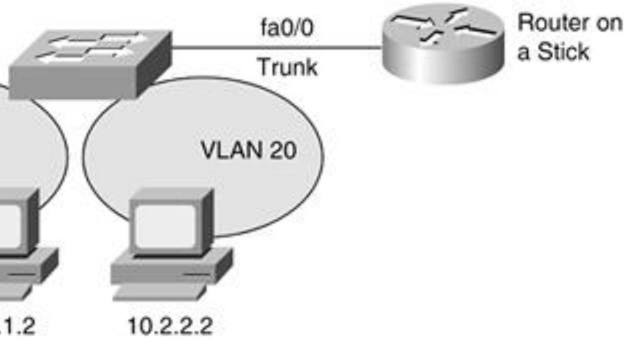
- A VLAN is a logical group of ports, usually belonging to a single IP subnet to control the size of the **broadcast domain**.
- Even though devices in different VLANs may be “**physically**” **connected**, as shown in the previous slides, these devices cannot communicate without the services of a default gateway, a router.
- Because VLANs isolate traffic to a defined broadcast domain and subnet, network devices in different **VLANs cannot communicate with each other without the use of a router**.
- This is known as **Inter-VLAN Routing**.

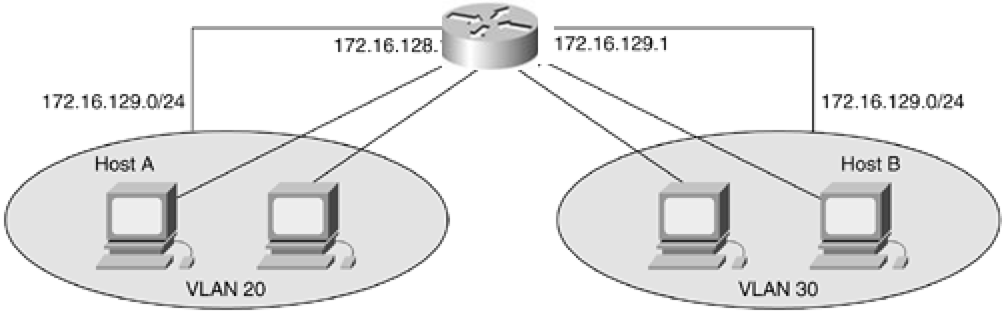
Inter-VLAN Routing

- The following devices are capable of providing inter-VLAN routing:
  - Any **Layer 3 multilayer Catalyst switch**
  - Any **external router** with an interface that supports **trunking** (router on a stick)
  - Any **external router** or group of routers with a **separate interface in each VLAN**

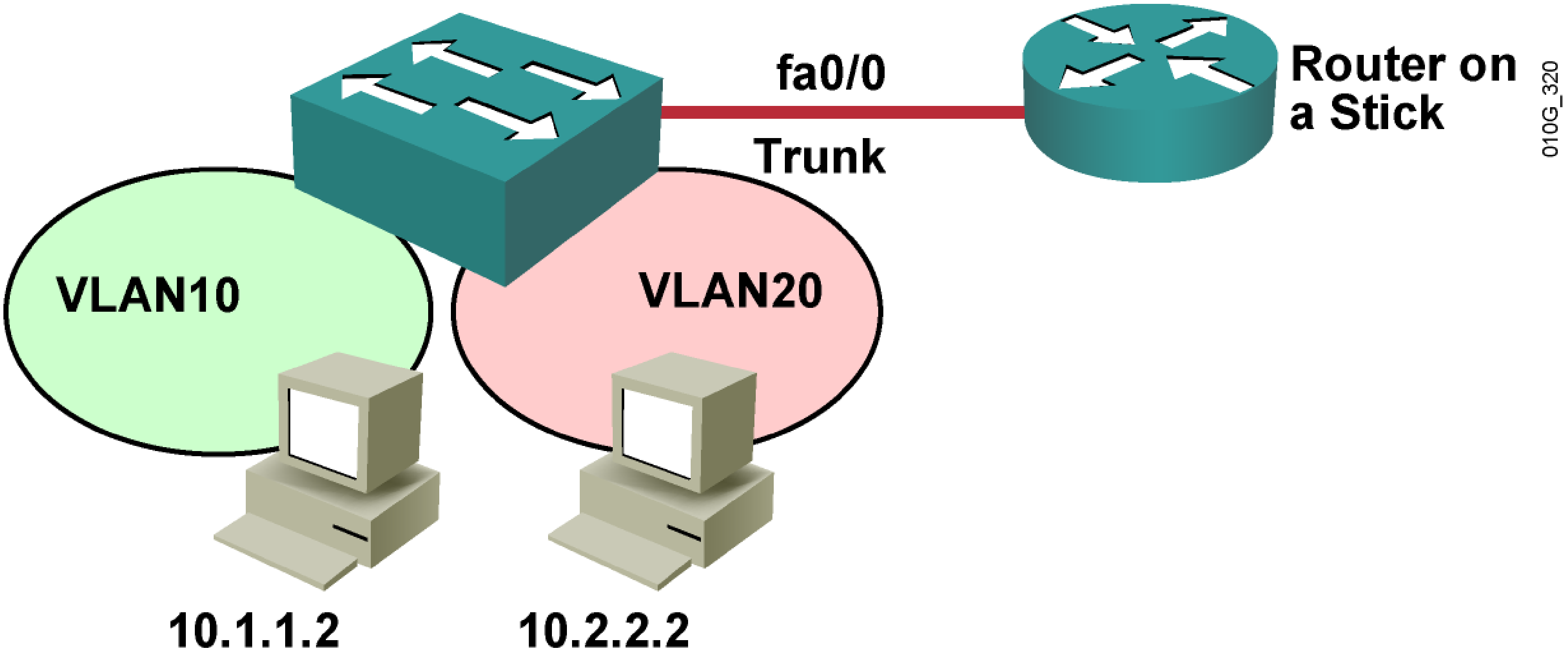


Or trunk port





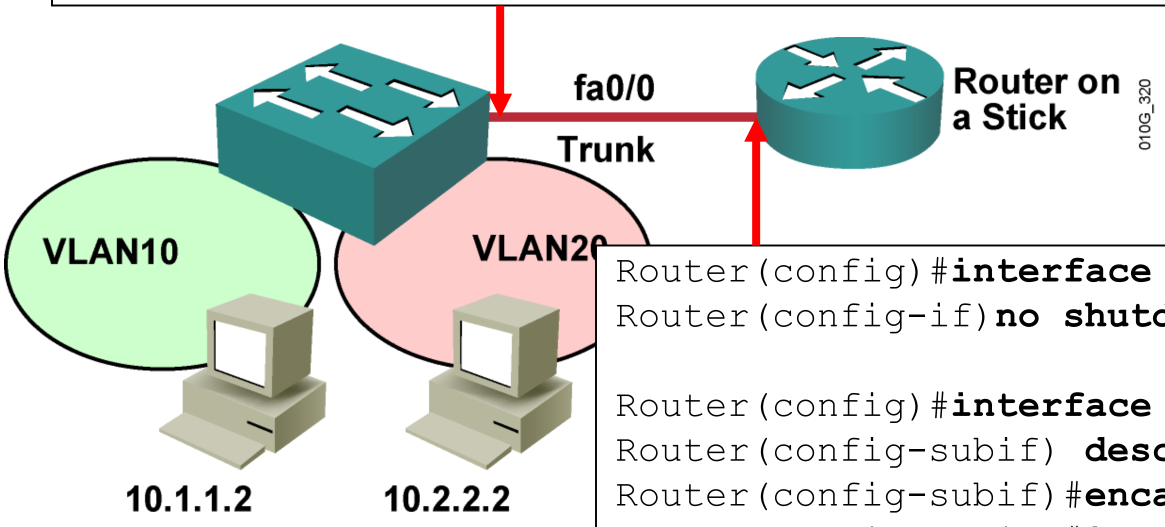
Inter-VLAN Routing with External Router



- Single trunk link carries traffic for multiple VLANs to and from router.

Router On A Stick: 802.1Q Trunk Link

```
switch(config)#interface FastEthernet 0/0
switch(config-if)#switchport trunk encapsulation dot1q
switch(config-if)#switchport mode trunk
```



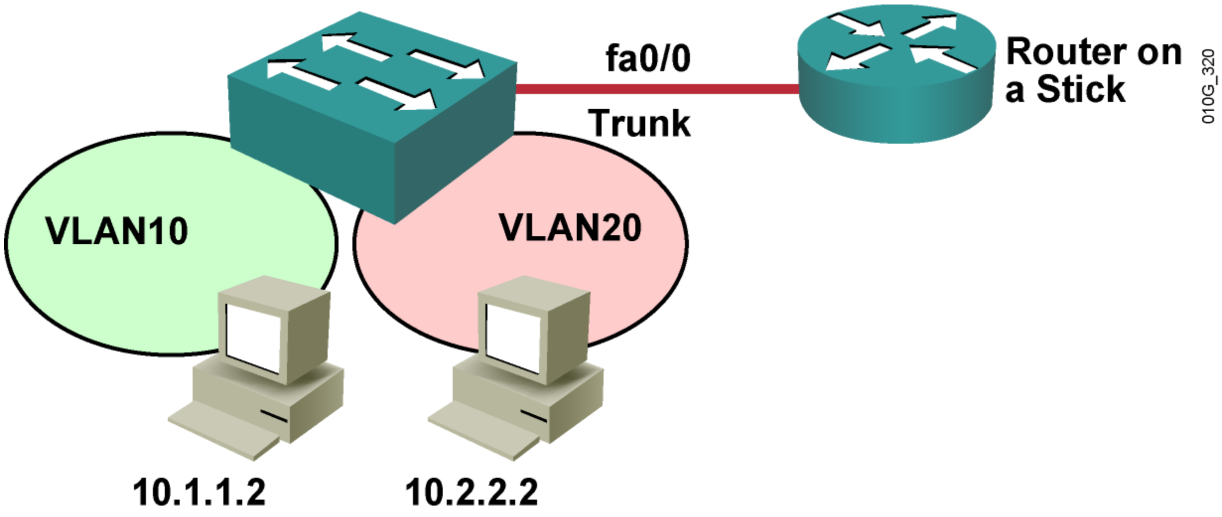
```
Router(config)#interface FastEthernet0/0
Router(config-if)no shutdown

Router(config)#interface FastEthernet 0/0.1
Router(config-subif) description VLAN 1
Router(config-subif)#encapsulation dot1Q 1 native
Router(config-subif)#ip address 10.10.1.1 255.255.255.0

Router(config)#interface FastEthernet 0/0.10
Router(config-subif) description VLAN 10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 10.10.10.1 255.255.255.0

Router(config)#interface FastEthernet 0/0.20
Router(config-subif)# description VLAN 20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 10.10.20.1 255.255.255.0
```

Router On a Stick

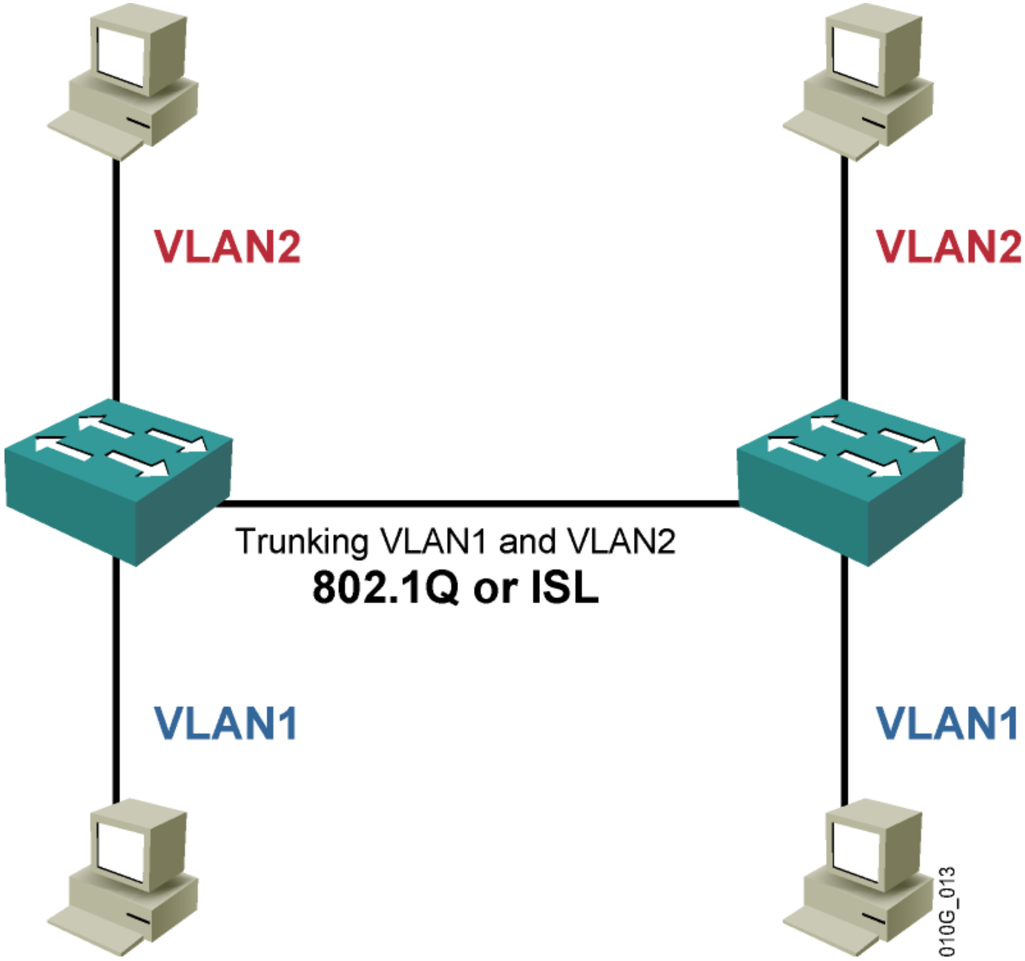


- Router on a stick is **very simple** to implement because routers are usually available in every network.
- Most enterprise networks use **multilayer switches** to achieve high packet-processing rates using hardware switching.
- **Multilayer (layer 3) switches** usually have packet-switching throughputs in the **millions of packets per second** (pps), whereas traditional **general-purpose routers** provide packet switching in the range of **100,000 pps to just over 1 million pps**.

Connecting VLANs with Multilayer Switches

Layer 2 Interfaces:

- ***Access port***— Carries traffic for a single VLAN
- ***Trunk port***— Carries traffic for multiple VLANs using Inter-Switch Link (ISL) encapsulation or 802.1Q tagging



Connecting VLANs with Multilayer Switches

Layer 2 Interfaces

```
DLSwitchA(config)#interface range fa 0/11 - 15
DLSwitchA(config-if-range)#switchport mode access
DLSwitchA(config-if-range)#switchport access vlan 10

DLSwitchA(config)#interface range fastethernet 0/1 - 4, gigabitethernet 0/2
DLSwitchA(config-if-range)#switchport trunk encapsulation dot1q
DLSwitchA(config-if-range)#switchport mode trunk
```

- Cisco IOS Switchport command
  - The `switchport` command configures an interface as a **Layer 2 interface**.
  - The `no switchport` command configures an interface as a **Layer 3 interface**.

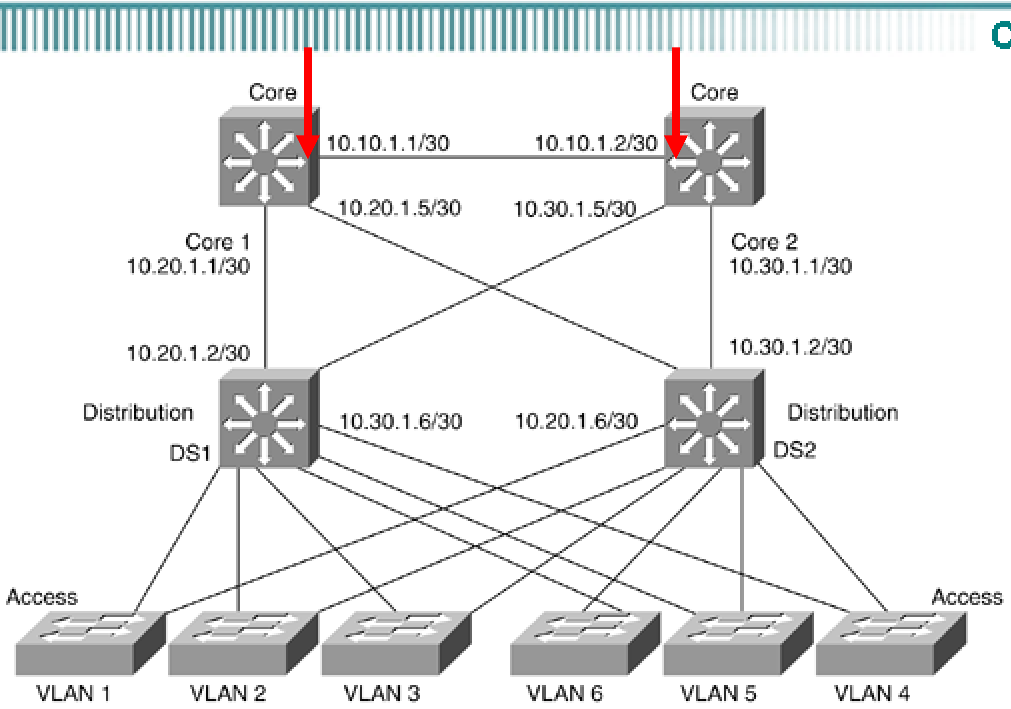
- Different models of Catalyst switches use different default settings for interfaces.
  - Catalyst 3550 and 4500 switches use Layer 2 interfaces by default
  - Catalyst 6500 family of switches (IOS) use Layer 3 interfaces by default.
  - Recall that default interface configurations do not appear in the configuration.

Layer 3 Interfaces

The Catalyst multilayer switches support three different types of **Layer 3 interfaces**:

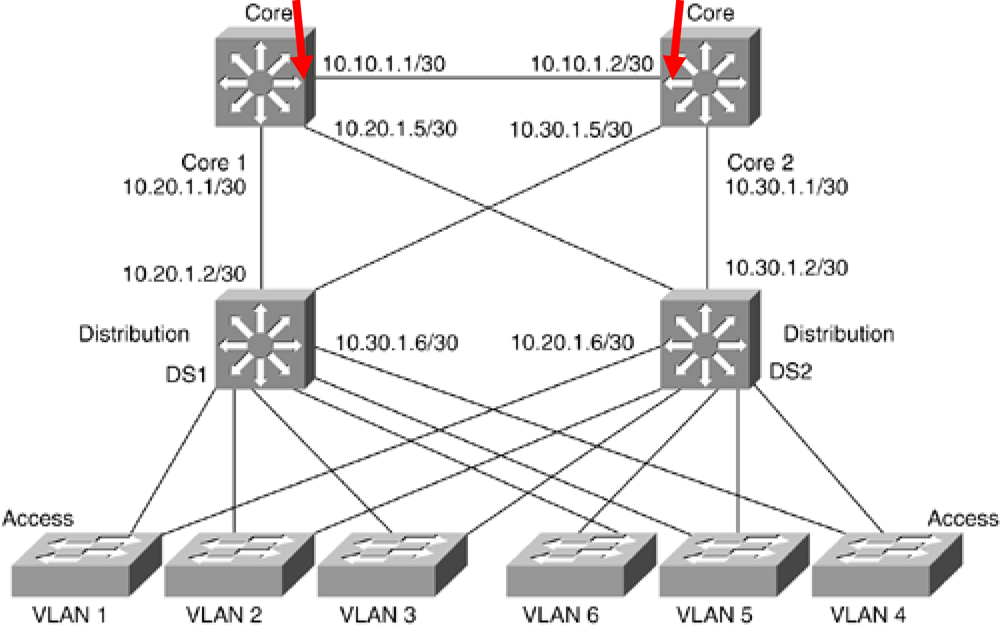
- ***Routed port***— A pure Layer 3 interface similar to a routed port on a Cisco IOS router.
- ***Switch virtual interface (SVI)***— A virtual VLAN interface for inter-VLAN routing. In other words, SVIs are the virtual routed VLAN interfaces.
- ***Bridge virtual interface (BVI)***— A Layer 3 virtual bridging interface. (Not discussed)

MLS Layer 3 Interface: Routed Port



- A routed port is a physical port that acts similarly to a port on a **traditional router** with Layer 3 addresses configured.
- Unlike an access port, a routed port is **not associated with a particular VLAN.**
- A routed port behaves like a regular router interface, except that it does ***not*** support **subinterfaces** as with Cisco IOS routers.

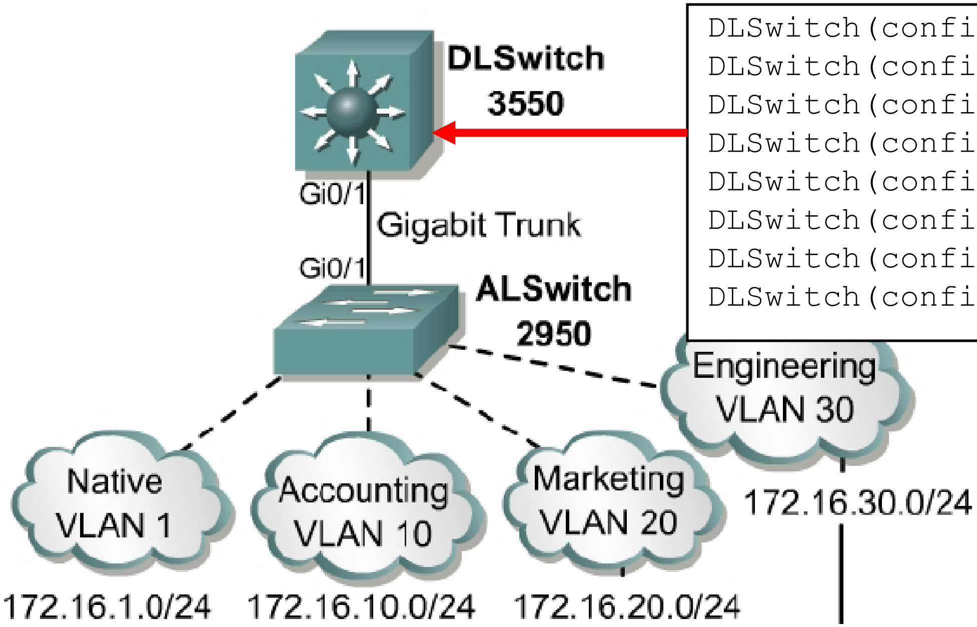
MLS Layer 3 Interface: Routed Port



```
Core-Left(config)#interface GigabitEthernet 1/1
Core-Left(config-if)#no switchport
Core-Left(config-if)#ip address 10.168.5.254 255.255.255.252

Core-Right(config)#interface GigabitEthernet 1/2
Core-Right(config-if)#ip address 10.168.6.254 255.255.255.252
% IP addresses may not be configured on L2 links.
Core-Right(config-if)#no switchport
Core-Right(config-if)#ip address 10.168.6.254 255.255.255.252
```

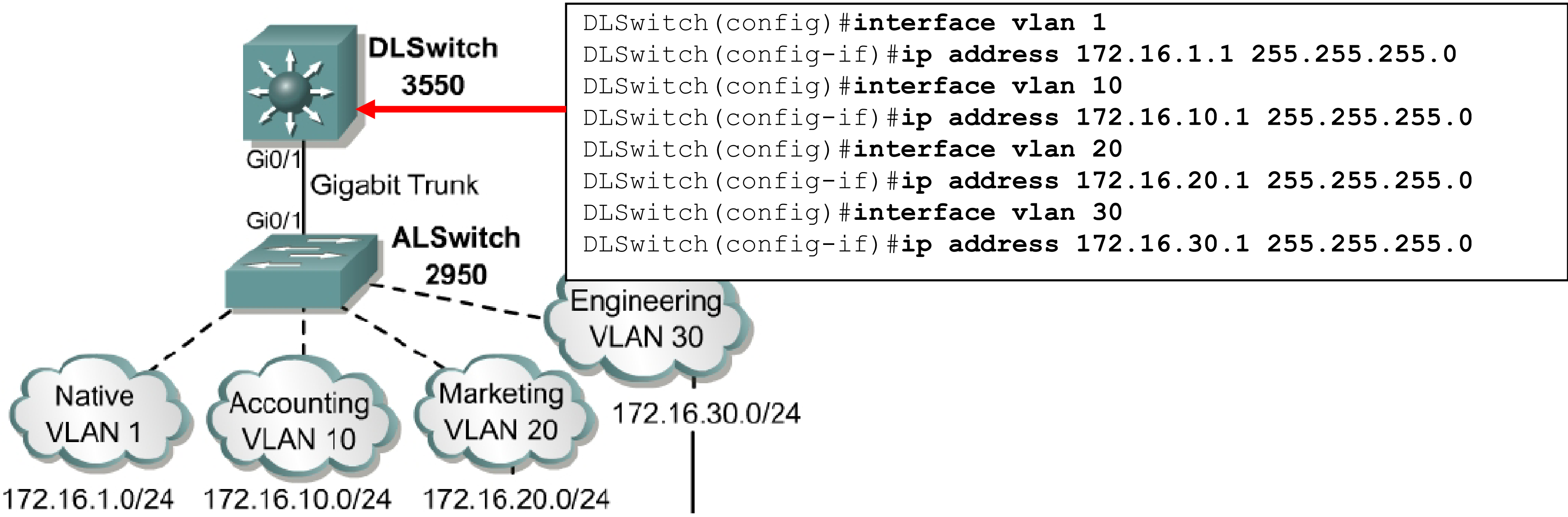
MLS Layer 3 Interface: SVI



```
DLSwitch(config)#interface vlan 1
DLSwitch(config-if)#ip address 172.16.1.1 255.255.255.0
DLSwitch(config)#interface vlan 10
DLSwitch(config-if)#ip address 172.16.10.1 255.255.255.0
DLSwitch(config)#interface vlan 20
DLSwitch(config-if)#ip address 172.16.20.1 255.255.255.0
DLSwitch(config)#interface vlan 30
DLSwitch(config-if)#ip address 172.16.30.1 255.255.255.0
```

- **Switch virtual interfaces (SVI)** are Layer 3 interfaces that are configured on multilayer Layer 3 Catalyst switches that are used for inter-VLAN routing.
- An SVI is a **virtual VLAN interface** that is associated with the **VLAN-ID** to enable **routing capability on that VLAN**.
- Note: *These are virtual interfaces!*

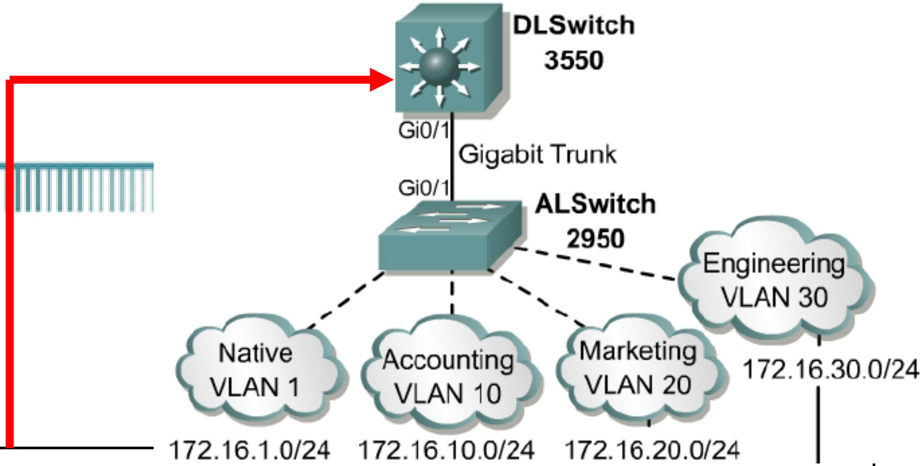
MLS Layer 3 Interface: SVI



```
DLSwitch(config)#interface vlan 1
DLSwitch(config-if)#ip address 172.16.1.1 255.255.255.0
DLSwitch(config)#interface vlan 10
DLSwitch(config-if)#ip address 172.16.10.1 255.255.255.0
DLSwitch(config)#interface vlan 20
DLSwitch(config-if)#ip address 172.16.20.1 255.255.255.0
DLSwitch(config)#interface vlan 30
DLSwitch(config-if)#ip address 172.16.30.1 255.255.255.0
```

- To configure communication between VLANs, you must configure each **SVI with an IP address and subnet mask** in the chosen address range for that subnet.
- The IP address associated with the VLAN interface is the **default gateway of the workstation.**

MLS Layer 3 Interface: SVI



```
DLSwitch(config)#interface vlan 1
DLSwitch(config-if)#ip address 172.16.1.1 255.255.255.0
DLSwitch(config)#interface vlan 10
DLSwitch(config-if)#ip address 172.16.10.1 255.255.255.0
DLSwitch(config)#interface vlan 20
DLSwitch(config-if)#ip address 172.16.20.1 255.255.255.0
DLSwitch(config)#interface vlan 30
DLSwitch(config-if)#ip address 172.16.30.1 255.255.255.0
```

- In this case, the **switch routes frames** from host on VLAN 10 to a host on VLAN 20 **directly on the switch via hardware switching without requiring an external router**.
- An SVI is mostly **implemented to interconnect the VLANs** on the Building Distribution submodules or the Building Access submodules in the multilayer switched network.

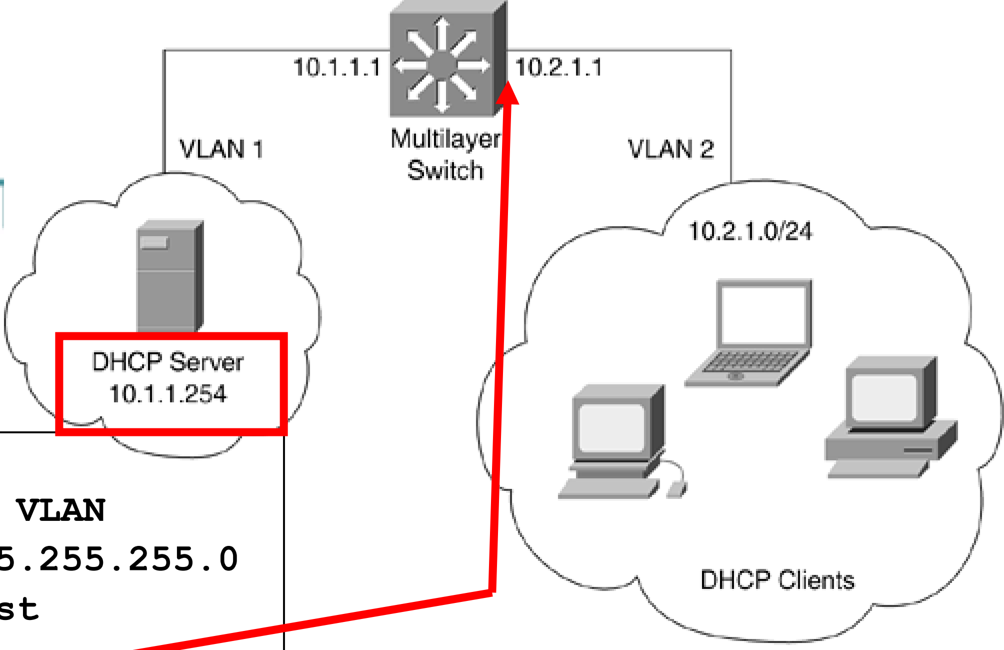
MLS Layer 3 Interface: BVI

- http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094663.shtml
- BVI.PDF
- A bridge virtual interface (BVI) is a Layer 3 virtual interface that acts like a normal SVI to route packets across bridged or routed domains. Bridging Layer 2 packets across Layer 3 interfaces is a legacy method of moving frames in a network. To configure a BVI to route, use the integrated routing and bridging (IRB) feature, which makes it possible to route a given protocol between routed interfaces and bridge groups within the same device. Specifically, routable traffic is routed to other routed interfaces and bridge groups, while local or unroutable traffic is bridged among the bridged interfaces in the same bridge group. As a result, bridging creates a single instance of spanning tree in multiple VLANs or routed subnets. This type of configuration complicates spanning tree and the behavior of other protocols, which in turn makes troubleshooting difficult.
- In today's network, however, bridging across routed domains is highly discouraged.

IP Broadcast Forwarding

- **IP broadcast forwarding** is necessary when using VLANs to centrally locate DHCP or other servers **where clients rely on broadcasts to locate or communicate with the services** running on the server.
- For example, **DHCP** requests are IP subnet broadcasts to the 255.255.255.255 address.
- **Routers do not route these packets by default**.
- However, Cisco routers and Layer 3 switches **can be configured to forward these DHCP and other UDP broadcast packets** to a unicast or directed broadcast address.
- The broadcast-forwarding features support more than DHCP and can forward any UDP broadcast.
- The following list summarizes the solutions that Cisco IOS IP broadcast forwarding features provide:
  - DHCP relay agent
  - UDP broadcast forwarding

DHCP Relay Agent

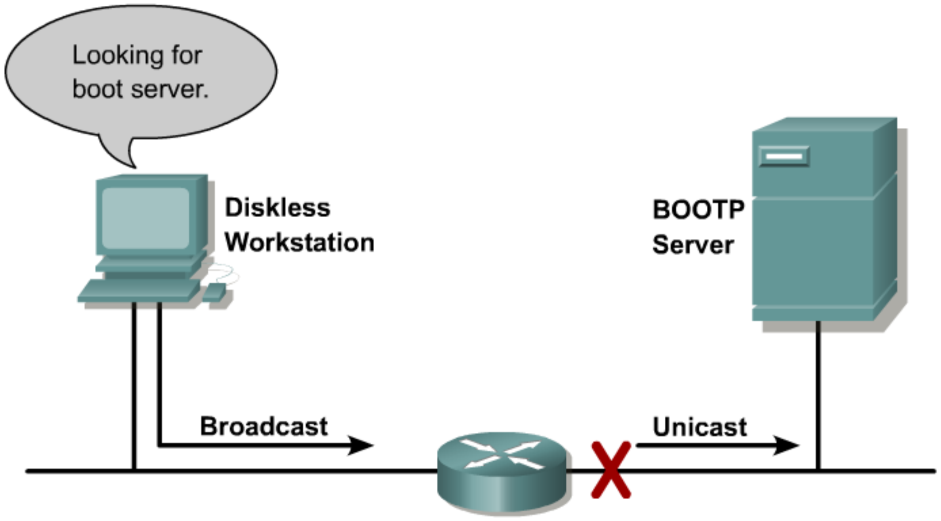


```
MLS(config)#interface vlan 1
MLS(configif)#description DHCP Server VLAN
MLS(config-if)#ip address 10.1.1.1 255.255.255.0
MLS(config-if)#no ip directed-broadcast

MLS(config)#interface vlan 2
MLS(config-ig)#description DHCP clients
MLS(config-if)#ip address 10.2.1.1 255.255.255.0
MLS(config-if)#no shutdown
MLS(config-if)#no ip directed-broadcast
MLS(config-if)#ip helper-address 10.1.1.254
```

- Because Layer 3 devices do not pass broadcasts by default, each subnet requires a DHCP server unless the routers are configured to forward the DHCP broadcast using the DHCP relay agent feature.
- To enable the **DHCP relay agent feature**, configure the **`ip helper-address`** command with the **DHCP server IP address** on the **client VLAN interfaces**. (For multiple DHCP servers, use multiple commands.)

DHCP Relay Agent (FYI)



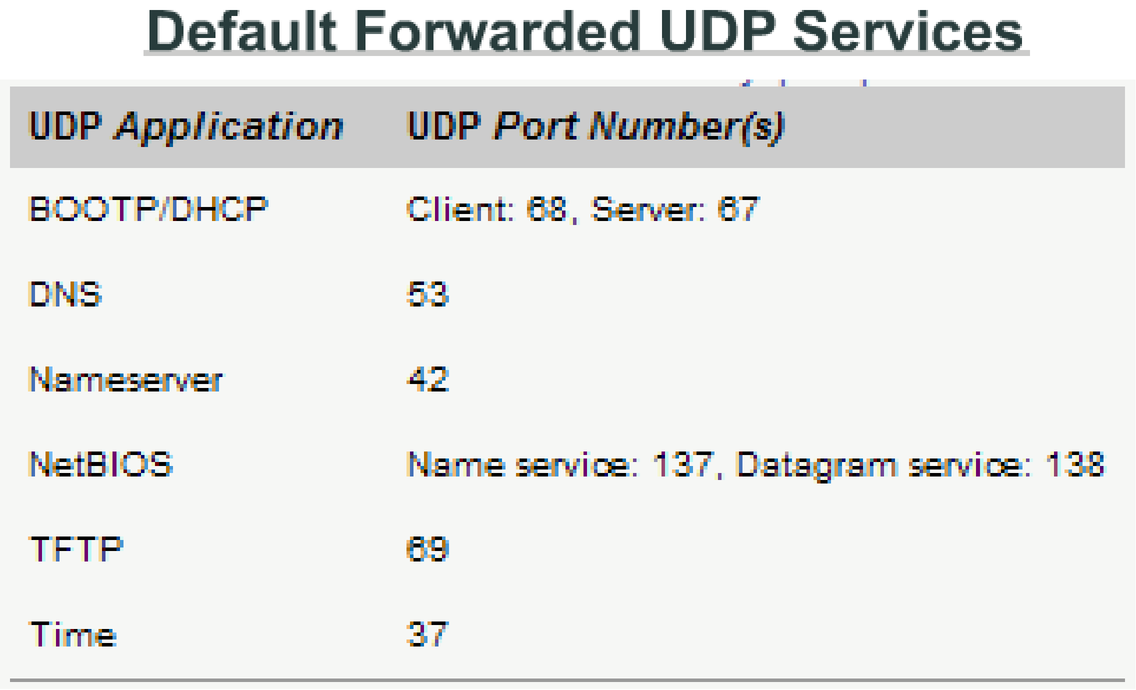
Routers do not forward broadcasts natively, but with the use of the **`ip helper-address`** command, broadcasts can be forwarded by the router to a specific server on another subnet.

- From Cisco.com:
- http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00804412bf.html
- The DHCP client broadcasts a request for an IP address and additional configuration parameters on its local LAN. Router B, acting as a DHCP relay agent, picks up the broadcast and generates a new DHCP message to send out on another interface. As part of this DHCP message, the relay agent inserts the IP address of the interface containing the **ip helper-address** command into the gateway IP address (giaddr) field of the DHCP packet. This IP address enables the DHCP server to determine which subnet should receive the offer and identify the appropriate IP address range to offer. The DHCP relay agent sends the local broadcast, via IP unicast, to the DHCP server address 172.16.1.2 specified by the **ip helper-address** interface configuration command.

DHCP Relay Agent

The *ip helper-address* command not only forwards DHCP UDP packets but also forwards TFTP, DNS, Time, NetBIOS, name server, and BOOTP packets by default.

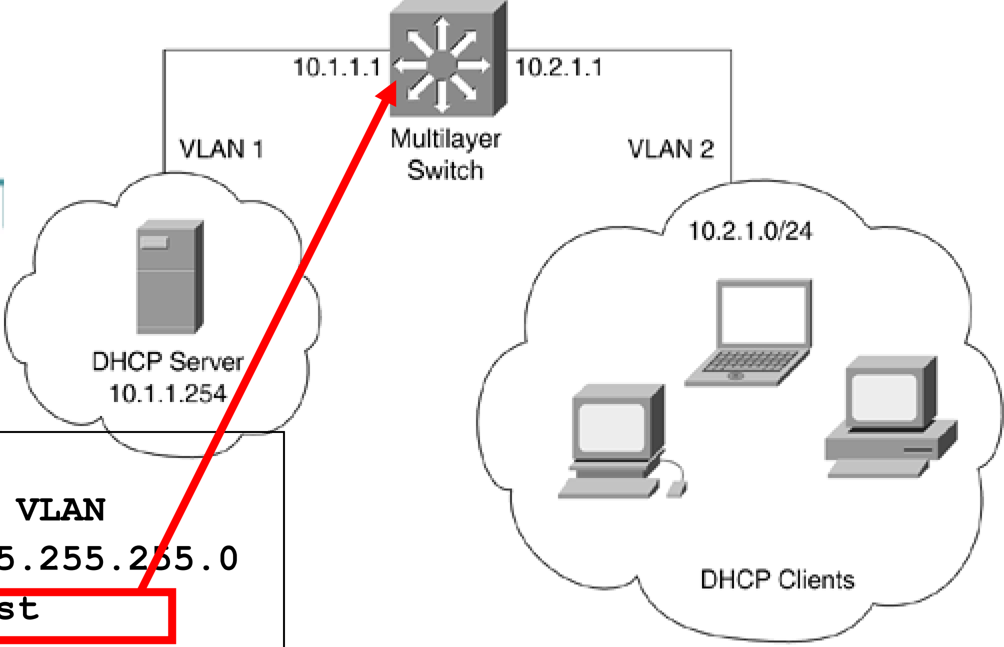
By default, the **ip helper-address** command forwards the eight UDPs services.



Default Forwarded UDP Services

UDP *Application*	UDP *Port Number(s)*
BOOTP/DHCP	Client: 68, Server: 67
DNS	53
Nameserver	42
NetBIOS	Name service: 137, Datagram service: 138
TFTP	69
Time	37

DHCP Relay Agent



```
MLS(config)#interface vlan 1
MLS(configif)#description DHCP Server VLAN
MLS(config-if)#ip address 10.1.1.1 255.255.255.0
MLS(config-if)#no ip directed-broadcast

MLS(config)#interface vlan 2
MLS(config-ig)#description DHCP clients
MLS(config-if)#ip address 10.1.2.1 255.255.255.0
MLS(config-if)#no shutdown
MLS(config-if)#no ip directed-broadcast
MLS(config-if)#ip helper-address 10.1.1.254
```

See Improving Security on Routers: http://www.cisco.com/warp/public/707/21.html

- When applying the **`ip helper-address`** command, make sure the **`ip directed-broadcast`** is ***not*** configured on any **outbound interfaces** that the UDP broadcast packets need to traverse.
- The **`no ip directed-broadcast`** command configures the router or switch to prevent the translation of a directed broadcast to a physical broadcast (MAC FF).
- This is a default behavior since Cisco IOS Release 12.0, implemented as a security measure.

UDP Broadcast Forwarding

```
Router(config)#interface vlan 1
Router(config-if)#ip address 10.100.1.1 255.255.255.0
Router(config-if)#ip helper-address 10.200.1.254

Router(config)#no ip forward-protocol udp netbios-ns
Router(config)#ip forward-protocol udp mobile-ip
```

- To specify additional UDP broadcasts for forwarding by the router when configuring the *ip helper-address* interface command, use the following global command:

  `ip forward protocol udp udp_ports`

- This is the configuration of **not** forwarding UDP broadcasts for the NetBIOS name service, a default behavior when configuring the *ip helper-address* command.
- This example also shows the configuration of forwarding UDP packets for mobile-ip and the other default UDP forwarded ports.

Inter-VLAN Routing

Cabrillo College

CIS 187 Multilayer Switched Networks

CCNP 3 version 4

Rick Graziani

Fall 2006